IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS

AARON JOHNSON, individually and on behalf of all others similarly situated; Plaintiff, v. **GRYPHON HEALTHCARE, LLC,** Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff Aaron Johnson ("Plaintiff") brings this Class Action Complaint against GRYPHON HEALTHCARE, LLC, ("Gryphon" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information (PII) and protected health information (PHI) (collectively, "Private Information"). Now, the Private Information is in the hands of cybercriminals who will use Plaintiff's and the Class's PII for an unlimited time.

2. Defendant Gryphon is a medical billing service that provides a variety of services to medical providers across the country.[1]

[1] https://www.Gryphonpros.com/About-Us/Default.aspx (last viewed October 17, 2024).

3. Defendant identified it was subject to a cyberattack in or about August 13, 2024 (the "Data Breach"). Defendant investigated the Data Breach and confirmed that an unauthorized actor accessed Defendant's systems on August 13, 2024, and obtained Plaintiff and the Class Members Private Information.[2] Although Gryphon concluded its investigation on September 3, 2024, it did not send notice to those potentially affected by its services until a month and a half later in October 2024. Defendant's notice confirms the cyber criminals obtained Plaintiff and the Class Members data and the data remains with such unauthorized criminals.

4. The Private Information was acquired by cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals. According to Defendant's report to the U.S. Department of Health and Human Services, 393,358 individuals' sensitive data was compromised.[3]

5. Plaintiff brings this class action lawsuit on behalf of himself and those similarly situated to address Defendant's inadequate safeguarding of Class Members' Personal Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information was likely accessed by an unknown third party and precisely what specific type of information was accessed.

6. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Personal Information was a known risk to Defendant and thus Defendant was on notice that failing to take

[2] *See* Defendant's Notice of Data Breach to Plaintiff, attached as Exhibit 1.
[3] U.S. Department of Health & Human Services Office for Civil Rights, *Cases Currently Under Investigation*, *available at* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (*last accessed* October 17, 2024).

steps necessary to secure the Personal Information from those risks left that information in a dangerous condition.

7. Because of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

8. By obtaining, collecting, using, and profiting from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the Private Information was obtained by criminals during the Data Breach.

9. The exposed Private Information of Plaintiff and Class Members can-and likely will-be sold on the dark web. Indeed, Plaintiff's and Class Members' Private Information has likely already been published on the dark web.

10. Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers—the gold standard for identity thieves.

11. This Private Information was compromised because of Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant has yet to contact affected individuals or the U.S. Department of Health and Human Services.

12. Plaintiff and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their lifetimes.

13. Plaintiff brings this action on behalf of all persons whose Private Information was

compromised because of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

14. Plaintiff and Class Members have suffered injury because of Defendant's conduct. These injuries include:

(i) lost or diminished value of Private Information;

(ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;

(iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, lost time; and

(iv) the continued and exacerbated to their Private Information which:

a. remains unencrypted and available for unauthorized third parties to access and abuse; and

b. may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

15. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded. Defendant further disregarded their rights by failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures for the encryption of data, even for internal use.

16. Because of the Data Breach, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe,

and they should be entitled to injunctive and other equitable relief.

PARTIES

17. Plaintiff Aaron Johnson is a Citizen of League City, Texas and intends to remain there throughout this litigation.

18. Defendant Gryphon Healthcare, LLC is a limited liability company that has its principal place of business in Harris County, Texas located at 25202 Northwest Freeway, Suite H Cypress, Texas. Upon information and belief, the membership of Gryphon is comprised of citizens and entities located in Texas. Nevertheless, diversity jurisdiction exists under CAFA, as discussed in the Jurisdiction Section of this Complaint, infra.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is at least 393,358 people Defendant reported to HHS, and at least minimal diversity exists because many of whom have different citizenship from Defendant, including 47 individuals who live in Maine.[4] Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has personal jurisdiction over Defendant because Gryphon operates, and is headquartered, in this District and conducts substantial business in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(l) because a substantial part of the events giving rise to this action occurred in this District. Defendant is also based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members from and/or in this District.

[4] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/07b59e7d-72e9-4bbe-abcb-dca588c27e65.html (Last viewed October 17, 2024).

FACTUAL ALLEGATIONS

Defendant's Business

22. Defendant provides revenue cycle, coding and compliance and consulting services for healthcare providers.[5]

23. Throughout this Complaint, all Defendant's locations will be referred to collectively as "Defendant."

24. In the ordinary course of receiving health care services from Defendant, each patient must provide (and Plaintiff did provide) Defendant with sensitive, personal, and private information, such as his or her:

- address;
- telephone number;
- date of birth;
- Social Security number;
- dates of service;
- diagnosis information;
- health insurance information;
- medical treatment information;
- prescription information;
- provider information; and
- medical record number.

25. name, date of birth, address, Social Security number, dates of service, diagnosis information, health insurance information, medical treatment information, prescription information, provider information and medical record numAll of Defendant's employees, staff, entities, sites, and locations may share patient information with each other for various purposes, as should be disclosed in a HIPAA compliant privacy notice ("Privacy Policy") that Defendant is required to maintain.

[5] https://www.gryphonhc.com/ (last viewed October 17, 2024).

26. Upon information and belief, Defendant's HIPAA Privacy Policy is provided to every patient prior to receiving treatment and upon request.

27. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws, including the Health Insurance Portability and Accountability Act ("HIPAA").

28. The patient and employee information held by Defendant in its computer system and network included the Private Information of Plaintiff and Class Members.

The Data Breach

29. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

30. On or around October 11, 2024, Defendant mailed a "Notice of Data Breach" to Plaintiff that states in part:

> **What Happened.** On August 13, 2024, Gryphon became aware of a data security incident involving a partner that Gryphon provides medical billing services for, which resulted in unauthorized access to certain personal and/or protected health information maintained by Gryphon. As a result of this incident, an unauthorized actor may have access certain files and data containing information relative to patients for whom Gryphon provides medical billing services.
> …
> **What Information was involved.** The information may have included your name, date of birth, address, Social Security number, dates of service, diagnosis information, health insurance information, medical treatment information, prescription information, provider information and medical record number.[6]

31. The U.S. Department of Health and Human Services requires, "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must

[6] *See* Exhibit 1.

notify the Secretary of the breach without unreasonable delay and in *no case later than 60 calendar days* from the discovery of the breach."[7] Further, if "the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate," and later provide an addendum or correction to HHS.[8]

32. Defendant's notice was dated October 11, 2024—more than two months after Defendant discovered the Data Breach. Furthermore, the notice does not inform Plaintiff how long her Private Information was insecure and in the hands of cybercriminals and/or if the information was recovered from the hackers. *See* Exhibit 1.

33. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

34. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

35. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches in the healthcare industry preceding the date of the breach.

36. In 2023, a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[9] Of the 2023 recorded data breaches, 809 of them, or 25%, were in the medical or healthcare industry.[10] The 809 reported

[7] U.S. Department of Health and Human Services, *Submitting Notice of a Breach to the Secretary* (Feb. 27, 2023) https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed October 17, 2024) (emphasis added).
[8] *Id.*
[9] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited October 17, 2024).
[10] *Id.*

breaches reported in 2023 exposed nearly 56 million sensitive records, compared to only 343 breaches that exposed just over 28 million sensitive records in 2022.[11]

37. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

38. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[12]

39. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

40. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

41. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[13] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting

[11] *Id*. at 11, Fig.3.
[12] Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, *Security Magazine* (Nov. 23, 2020), *available at* https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited October 17, 2024).
[13] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited October 17, 2024).

someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[14]

42. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions also clarify the measures businesses must take to meet their data security obligations.

44. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

45. Defendant failed to properly implement basic data security practices.

46. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

[14] *Id.*

47. Defendant was always fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

48. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

49. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including, but not limited to, educating all employees; using strong passwords; creating multi-layer security, including firewalls, antivirus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data; and limiting which employees can access sensitive data.

50. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

51. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including, without limitation, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

52. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Conduct Violates HIPAA and Reveals its Insufficient Data Security

53. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

54. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

55. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a) (1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

56. A Data Breach such as the one Defendant experienced is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule. *See* 45 C.F.R. 164.402 (Defining "Breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information.").

57. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to meet standards mandated by HIPAA regulations.

DEFENDANT'S BREACH

58. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules related to individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures about PHI as necessary and appropriate for the members of its

workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304, definition of "encryption").

59. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

60. Plaintiff and Class Members now face an increased risk of fraud and identity theft.

DATA BREACHES PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

61. Data Breaches such as the one experienced by Defendant's patients are especially problematic because of the disruption they cause to the daily lives of victims affected by the attack.

62. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[15]

63. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (possibly an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent

[15] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (last visited October 17, 2024) ("GAO Report").

charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[16]

64. Identity thieves use stolen personal information such as Social Security numbers for various crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

65. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

66. Theft of Private Information is gravely serious. PII/PHI is a valuable property right.[17] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

67. Theft of PHI is also gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[18] Drug manufacturers, medical device

[16] Federal Trade Commission, *What To Do Right Away* (2024), *available at* https://www.identitytheft.gov/Steps (last visited October 17, 2024).
[17] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[18] *See* Federal Trade Commission, *Medical Identity Theft*, *available at* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited October 17, 2024).

manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

68. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

69. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

70. There is a strong probability that all the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

71. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[19] PII is particularly valuable because criminals can use it to target victims

[19] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited October 17, 2024).

with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

72. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for more credit lines.[20] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[21] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

73. It is also hard to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[22]

74. Healthcare data, as one would expect, demands an exceptionally high price on the black market. The National Association of Healthcare Access Management reports, "[p]ersonal medical data is said to be more than ten times as valuable as credit card information."[23]

---

[20] Social Security Administration, *Identity Theft and Your Social Security Number* (2018), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited October 17, 2024).
[21] *Id* at 4.
[22] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (February 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited October 17, 2024).
[23] Laurie Zabel, *The Value of Personal Medical Information: Protecting Against Data Breaches*, NAHAM Connections, *available at* https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information (last visited October 17, 2024).

75. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $300 and up.[24]

76. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFF'S EXPERIENCE

77. Plaintiff Aaron Johnson is and at all times mentioned herein was an individual citizen of Texas, residing in the city of League City.

78. Plaintiff provided Defendant with his sensitive PII and PHI to receive healthcare services from Defendant. Plaintiff received notice of the Data Breach around Ocobter 11, 2024, informing him that his sensitive information was part of Defendant's Data Breach.

79. Plaintiff is careful about sharing his sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

80. Plaintiff stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his sensitive online accounts.

[24] Paul Ducklin, *FBI "ransomware warning" for healthcare is a warning for everyone!*, Sophos (Oct. 29, 2020) *available at* https://news.sophos.com/en-us/2020/10/29/fbi-ransomware-warning-for-healthcare-is-a-warning-for-everyone/ (last visited October 17, 2024).

81. Had Plaintiff been aware that Defendant's computer systems were not secure, he would not have entrusted his personal data to Defendant.

82. Because of the Data Breach, Defendant advised Plaintiff to take certain steps to protect his Private Information and otherwise mitigate his damages.

83. Because of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. This time was spent at Defendant's direction by way of the Data Breach notice where Defendant recommended that Plaintiff mitigate his damages by, among other things, monitoring his accounts for fraudulent activity.

84. Even with the best response, the harm caused to Plaintiff cannot be undone.

85. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

86. Plaintiff has suffered imminent and impending injury arising from the exacerbated risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

87. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

88. To date, Defendant has done absolutely nothing to compensate Plaintiff and Class Members for the damages they sustained in the Data Breach.

89. Defendant's failure to compensate is wholly inadequate as it fails to make whole all victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it provides no compensation for its unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

90. Furthermore, Defendant's advice to Plaintiff and Class Members places the burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

91. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

92. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

93. Plaintiff was damaged in that her Private Information is in the hands of cyber criminals.

94. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

95. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

96. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

97. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

98. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

99. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

100. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

101. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

102. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

103. Further, because of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

104. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ALLEGATIONS

105. Plaintiff brings this nationwide class action on behalf of himself and on behalf of

others similarly situated under Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

106. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> **All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach (the "Class").**

107. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; all federal, state, or local governments, including, but not limited to, their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

108. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

109. Numerosity, Fed R. Civ. P. 23(a)(l): Class Members are so Many that joinder of all members is impracticable. Upon information and belief, there exceed 5,941 individuals[25] whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

110. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

[25] https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last viewed September 30, 2024).

b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. When Defendant learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages because of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution because of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced because of the Data Breach.

111. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised because of the Data Breach, because of Defendant's misfeasance.

112. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the

Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged here apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct toward the Class as a whole, not on facts or law applicable only to Plaintiff.

113. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

114. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged here; it will permit many Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

115. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure

to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

116. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

117. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

118. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

119. And Defendant has acted or refused to act on grounds generally applicable to the Classes and thus final injunctive or corresponding declaratory relief for the Class Members is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

120. Likewise, issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members; and

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief because of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Putative Rule 23 Class)

121. Plaintiff and the Class repeat and re-allege every allegation as if fully set forth herein.

122. Plaintiff and the Class entrusted Defendant with their Private Information.

123. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

124. Defendant knows about the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

125. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

126. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class Members in Defendant's possession was adequately secured and protected.

127. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under regulations.

128. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

129. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

130. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

131. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly given Defendant's inadequate security practices.

132. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

133. Defendant's own conduct created a foreseeable risk of harm. to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach asset forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

134. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

135. Defendant was able to protect against the harm suffered by Plaintiff and the Class because of the Data Breach.

136. Defendant had and continue to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Info by third parties.

137. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

138. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

139. Defendant, through its actions and/or omissions, unlawfully breached its duties to

Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

140. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

141. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of theft.

142. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

143. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information it was no longer required to retain under regulations.

144. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

145. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Private Information of Plaintiff and the Class would not have been compromised.

146. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure

to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

147. Additionally, Section 5 of the FTC Act prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

148. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as detailed herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

149. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se.*

150. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

151. The harm attributable to the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, because of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

152. As a direct and proximate result of Defendant's negligence and negligence *per se,* Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or

unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiff and the Class.

153. As a direct and proximate result of Defendant' negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

154. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

155. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have a right to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF THIRD PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiff and the Putative Rule 23 Class)

156. Plaintiff and the Class repeat and re-allege every allegation as if fully set forth herein.

157. Gryphon entered into various contracts with its financial and staffing clients to provide software, payroll, and other services. As a material part of those contracts Defendant agreed to implement reasonable data security practices and procedures sufficient to safeguard the PII and PHI provided to it by its clients.

158. These contracts are virtually identical to each other and the provisions regarding PII and PHI were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that Gryphon agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII and PHI belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

159. Gryphon knew that if it were to breach these contracts with its staffing and financial clients, its consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their Private Information

160. Gryphon breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' Private Information.

161. As a reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Gryphon's failure to use reasonable data security measures to store their PII and PHI, including but not limited to, the actual harm sustained from the loss of their Private Information to cybercriminals.

162. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Putative Rule 23 Class)

163. Plaintiff and the Class repeat and re-allege every allegation as if fully set forth herein.

164. This Count is pled in the alternative to Count II herein.

165. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information.

166. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

167. Rather than provide a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by using cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

168. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

169. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

170. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

171. Plaintiff and Class Members have no adequate remedy at law.

172. As a direct and proximate result of Defendant's conduct, Plaintiff and Class

Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession and (vii) future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiff and Class Members.

173. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

174. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

a. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

c. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including, but not limited to, an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class

Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employee's compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

d. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f. For prejudgment interest on all amounts awarded; and

g. Any other relief that this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands this matter be tried before a jury.

Date: October 17, 2024,

Respectfully submitted,

/s/ Leigh S. Montgomery
EKSM, LLP
Leigh S. Montgomery
Texas Bar No. 24052214
lmontgomery@eksm.com
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

ATTORNEYS FOR PLAINTIFF